

PTO/SB/21 (08-03)

Approved for use through 07/31/2008. CMB 0851-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>TRANSMITTAL FORM</b> (to be used for all correspondence after initial filing)		Application Number	09/650,712
		Filing Date	8/20/2000
		First Named Inventor	Rico Mariani
		Group Art Unit	2131
		Examiner Name	SHIN HON CHEN
Total Number of Pages in This Submission		Attorney Docket Number	MS1-578US
<b>ENCLOSURES (check all that apply)</b>			
<input checked="" type="checkbox"/> Fee Transmittal Form <input type="checkbox"/> Fee Attached  <input type="checkbox"/> Amendment / Reply <input type="checkbox"/> After Final <input type="checkbox"/> Affidavits/declaration(s) <input checked="" type="checkbox"/> Extension of Time Request <input type="checkbox"/> Express Abandonment Request <input type="checkbox"/> Information Disclosure Statement <input type="checkbox"/> Certified Copy of Priority Documents <input type="checkbox"/> Response to Missing Parts/Incomplete Application  <input type="checkbox"/> Response to Missing Parts under 37 CFR 1.52 or 1.53	<input type="checkbox"/> Drawing(s) <input type="checkbox"/> Licensing-related Papers <input type="checkbox"/> Petition <input type="checkbox"/> Petition to Convert to a Provisional Application <input type="checkbox"/> Power of Attorney, Revocation <input type="checkbox"/> Change of Correspondence Address <input type="checkbox"/> Terminal Disclaimer <input type="checkbox"/> Request for Refund <input type="checkbox"/> CD, Number of CD(s)	<input type="checkbox"/> After Allowance Communication to Group <input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences <input checked="" type="checkbox"/> Appeal Communication to Group (Appeal Notice, Brief, Reply Brief) <input type="checkbox"/> Proprietary Information <input type="checkbox"/> Status Letter <input type="checkbox"/> Other Enclosure(s) (please identify below):	Remarks
<b>SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT</b>			
Firm or Individual Name	Keyla D. Brant, Reg. No. 46576		
Signature	<i>Keyla D. Brant</i>		
Date	6/21/05		

<b>CERTIFICATE OF TRANSMISSION/MAILING</b>		
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.		
Typed or printed name	Carly Taylor	
Signature	<i>Carly Taylor</i>	Date 6/21/05

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

RECEIVED  
CENTRAL FAX CENTER

JUN 21 2005

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. ....09/650,712  
Filing Date ..... 08/29/2000  
Inventorship ..... Mariani, Rico  
Applicant ..... Microsoft Corporation  
Group Art Unit ..... 2131  
Examiner ..... Chen, Shin Hon  
Attorney's Docket No. .... MS1-0579US  
Title: Systems and Methods for Limiting Access to Potentially Dangerous Code

APPEAL BRIEF

To: Board of Patent Appeals and Interferences  
Alexandria, VA 22313-1450

From: Kayla D. Brant Tel. 509-324-9256 ext. 242  
Fax 509-323-8979  
Customer # 22801

Pursuant to 37 C.F.R. § 41.37 and 37 C.F.R. § 1.136(a), Applicant hereby submits a supplemental appeal brief for application 09/650,712 within four months from the filing date of the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

lee@hayes

1

60970.DOC

PAGE 4/28 \* RCVD AT 6/21/2005 2:20:36 PM [Eastern Daylight Time] \* SVR:USPTO-EFAXF-1/5 \* DHIS:8729306 \* CSID:509 323 8979 \* DURATION (mm-ss):06-48

TABLE OF CONTENTS

**Appeal Brief Items**

**Page**

(1)	Real Party in Interest	3
(2)	Related Appeals and Interferences	3
(3)	Status of Claims	3
(4)	Status of Amendments	4
(5)	Summary of Claimed Subject Matter	4
(6)	Grounds of Rejection to be Reviewed on Appeal	6
(7)	Argument	7
(8)	Claims Appendix	20

1       **(1) Real Party in Interest**

2       The real party in interest is the Microsoft Corporation, the assignee of all  
3       right and title to the subject invention.

4  
5       **(2) Related Appeals and Interferences**

6       There are no related appeals or interferences.

7  
8       **(3) Status of Claims**

9       Claims 1-10, 17-23, 27, 28, 30-32, and 34 are pending in this Application,  
10       and are set forth in the Appendix of Appealed Claims on page 20. Claims 1-10,  
11       17-23, 27, 28, 30-32, and 34 stand rejected. Claims 1-35 were originally filed in  
12       the Application. Claims 11-16, 24-26, 29, 33, and 35 were cancelled, and claims  
13       7-10, 17, 27, 30, and 32 were amended in an amendment filed July 29, 2004. No  
14       claims have been allowed.

15       Claims 1-10, 17-23, 27, 28, 30-32, and 34 are subject to this appeal and  
16       stand rejected as set forth in a Final Office Action dated January 11, 2005.  
17       Specifically:

18       Claims 1, 2, 5, 7-10, 17, 18, and 20-23 are rejected under  
19       35 U.S.C. § 102(e) as being clearly anticipated by U.S. Patent 6,499,109 issued to  
20       Balasubramaniam et al. (hereinafter, "Bal") (1/11/2005 Office Action p.2).

21       Claim 3 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal  
22       in view of U.S. Patent No. 6,499,105 issued to Yoshiura (hereinafter, "Yoshiura")  
23       and further in view of U.S. Patent No. 6,058,482 issued to Liu (hereinafter, "Liu")  
24       (1/11/2005 Office Action p.5).

25       Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal

1 in view of Yoshiura (1/11/2005 Office Action p.6).

2 Claim 6 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal  
3 in view of U.S. Patent No. 6,615,088 issued to Myer et al. (hereinafter, "Myer")  
4 (1/11/2005 Office Action p.6).

5 Claims 19, 32, and 34 are rejected under 35 U.S.C. § 103(a) as being  
6 unpatentable over Bal in view of Renaud (1/11/2005 Office Action p.8).

7 Claims 27, 28, 30, and 31 are rejected under 35 U.S.C. § 103(a) as being  
8 unpatentable over Bal in view of Liu (1/11/2005 Office Action p.9).

9  
10 **(4) Status of Amendments**

11 A rejection to claims 1-35 was issued on May 6, 2004 whereupon  
12 Applicant responded to address the Examiner's rationale for the rejection and to  
13 cancel claims 11-16, 24-26, 29, 33, and 35 and amend claim 7-10, 17, 27, 30,  
14 and 32. The claim amendments were entered, and subsequently, a final rejection  
15 was issued on January 11, 2005. A Notice of Appeal was filed on  
16 March 18, 2005. No amendments have been filed subsequent to the Examiner's  
17 final rejection dated January 11, 2005.

18  
19 **(5) Summary of Claimed Subject Matter**

20 Following is a concise explanation of each independent claim 1, 7, 17, 27,  
21 and 32 involved in the Appeal which includes specification references and  
22 exemplary drawing reference characters. As explained, the independent claims are  
23 not limited solely to the elements identified by the reference characters.

1 The claimed subject matter is directed to authenticating a digital signature  
2 associated with a web page prior to executing a least a portion of the web page.  
3 Specifically:

4  
5 Claim 1 includes associating a digital signature (226) with a web  
6 page (212); and delivering the web page (212) to an electronic device (204).

7  
8 Claim 7 describes receiving a web page (212') having a digital  
9 signature (226') that can be used to identify a source of the web page.  
10 (*Application, pg. 14, lines 11-12; Figure 3, block 308.*) The web page (212')  
11 contains executable script (216') that, when executed invokes a control  
12 object (218'). (*Application, pg. 12, lines 5-7.*) The web page is displayed and the  
13 control object invoked only if the source of the web page is determined to be  
14 authentic based on the digital signature associated with the web page.  
15 (*Application, pg. 15, lines 14-19.*)

16  
17 Claim 17 describes a computer system (204) that includes a web  
18 browser (230) for accessing a web page (212') that has an associated digital  
19 signature (226'), a processor (227) configured to execute script (216') that may be  
20 contained in the web page (212'), an executable control object (218') that may be  
21 invoked by the script in the web page, and a confirmation module (220')  
22 configured to authenticate the digital signature to determine, based on authenticity  
23 of the digital signature, whether the control object should be invoked.  
24 (*Application, pg. 13, lines 8-18; Figure 2, Client Computer 204.*)

1        Claim 27 describes a web browser (230) that determines if a received web  
2 page (212') contains instructions to invoke a control object (218') and determines  
3 if the web page has an associated digital signature (226'). If the web page has an  
4 associated digital signature, the browser authenticates the web page using the  
5 digital signature, and invokes the control object if the source of the web page is  
6 authenticated. (*Application, pg. 14, line 11-pg. 15, line 19.*)

7  
8        Claim 32 describes a control object (218') that authenticates a web  
9 page (212') that invokes the control object. The authentication is performed based  
10 on a digital signature (226') associated with the web page. A data-handling task is  
11 performed on the computer if the web page is determined to be authentic.  
12 (*Application, pg. 13, lines 1-7.*)

13  
14        (6) Grounds of Rejection to be Reviewed on Appeal

15        Claims 1, 2, 5, 7-10, 17, 18, and 20-23 are rejected under  
16 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,499,109 issued to  
17 Balasubramaniam et al. (hereinafter, "Bal") (*1/11/2005 Office Action p.2*).

18        Claim 3 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal  
19 in view of U.S. Patent No. 6,499,105 issued to Yoshiura (hereinafter, "Yoshiura")  
20 and further in view of U.S. Patent No. 6,058,482 issued to Liu (hereinafter, "Liu")  
21 (*1/11/2005 Office Action p.5*).

22        Claim 4 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal  
23 in view of Yoshiura (*1/11/2005 Office Action p.6*).  
24  
25

1 Claim 6 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Bal  
2 in view of U.S. Patent No. 6,615,088 issued to Myer et al. (hereinafter, "Myer")  
3 (1/11/2005 Office Action p.6).

4 Claims 19, 32, and 34 are rejected under 35 U.S.C. § 103(a) as being  
5 unpatentable over Bal in view of Renaud (1/11/2005 Office Action p.8).

6 Claims 27, 28, 30, and 31 are rejected under 35 U.S.C. § 103(a) as being  
7 unpatentable over Bal in view of Liu (1/11/2005 Office Action p.9).

8  
9 **(7) Argument**

10 Claims 1, 2, 5, 7-10, 17, 18, and 20-23 are not anticipated by Bal.

11  
12 Claims 1, 2, and 5

13 Bal describes verifying the source of software downloaded from a remote  
14 site to a client computer over a computer network before the software can be  
15 executed on the client computer. (Bal, Abstract.) Specifically, Bal describes a  
16 computer-executable program code that first determines the URL to which a  
17 browser running on the client computer is pointed and enables the downloaded  
18 software program only if the URL to which the browser is pointed is an authorized  
19 URL. (Bal, Summary.) Bal is akin to a scenario Applicant describes in the  
20 Background section that is improved with the claimed technique.  
21  
22  
23  
24  
25



1 Independent claim 1 recites:

2  
3 A method, comprising:

4 associating a digital signature with a web page; and

5 delivering the web page to an electronic device capable of  
6 authenticating the digital signature and executing at least a portion of  
7 the web page after the digital signature is authenticated.  
8

9  
10 In contrast to the method of claim 1, Bal describes examining a URL to  
11 which a browser is pointed to determine whether or not to allow execution of  
12 downloaded software. Bal does not describe "associating a *digital signature with*  
13 *a web page*," nor does Bal describe "delivering the web page to an electronic  
14 device capable of *authenticating the digital signature* and executing at least a  
15 portion of the web page after the digital signature is authenticated," as claimed.  
16 The Office cites Bal, column 7, lines 32-38 as describing "associating a digital  
17 signature with a web page." (1/11/2005 Office Action p.2) However, the cited  
18 portion of Bal (column 7, lines 32-38) states, "initiating the downloading of a web  
19 page on the browser window on the client computer based on the URL, wherein  
20 the web page has associated therewith a control software program with a  
21 corresponding digital signature; verifying the control software program using the  
22 digital signature." This portion of Bal clearly states that a digital signature is  
23 associated with the control software program – *not* with the web page, as found in  
24  
25

1 claim 1. Furthermore, Bal, claim 1, of which the cited language is a portion, goes  
2 on to recite, "querying the browser program to determine the URL to which the  
3 browser program is pointed; determining whether the URL to which the browser  
4 program is pointed is authorized; executing the control software program if it is  
5 determined that *the URL to which the browser program is pointed* is authorized."

6 Bal describes executing downloaded software based on authentication of a URL to  
7 which a browser program is pointed. Bal does not describe executing at least a  
8 portion of the web page after the digital signature is authenticated, where the  
9 digital signature is associated with the web page, as recited in claim 1.

10 Accordingly, claim 1 is allowable over Bal.

11  
12 Claims 2 and 5 are allowable by virtue of their dependency on claim 1.

13 Claims 7-10

14 Independent claim 7 recites:

15  
16 A method, comprising:

17 receiving a web page from a server, the web page containing  
18 executable script that, when executed, invokes a control object, the  
19 web page having a digital signature that can be used to identify a  
20 source of the web page;

21 determining whether the source of the web page is authentic  
22 via the digital signature; and  
23 in an event that the source of the web page is authentic,  
24 displaying the web page and invoking the control object  
25

1 In contrast to claim 7, Bal describes verifying a URL associated with a web  
2 page, and executing a control software program only after verification of the URL.  
3 (Bal, column 7, lines 26-51 – claim 1.) As stated above with reference to claim 1,  
4 Bal does not describe “a web page having a digital signature that can be used to  
5 identify a source of the web page,” as claimed. Accordingly, claim 7 is allowable  
6 over Bal.

7 Claims 8-10 are allowable by virtue of their dependency on claim 7.

8  
9 Claims 17, 18, and 20-23

10 Independent claim 17 recites:

11  
12 A system, comprising:

13 a web browser configured to access a web page having a  
14 digital signature;

15 a processor configured to execute script contained in the web  
16 page;

17 an executable control object that may be invoked by the  
18 script in the web page and is executable on the processor; and

19 a confirmation module configured to authenticate the digital  
20 signature to determine based on authenticity of the digital  
21 signature, whether the control object should be invoked.

22  
23 In contrast to claim 7, Bal describes authenticating a digital signature  
24 associated with a control software program and verifying a URL associated with a  
25

web page, to determine whether to execute the control software program. (Bal, column 7, lines 26-51 – claim 1.) As stated above with reference to claim 1, Bal does not describe “a web page having a digital signature,” as claimed. Furthermore, Bal does not describe authenticating the digital signature associated with the web page to determine whether the control object should be invoked. Rather, Bal describes verifying a URL associated with the web page to determine whether a control object should be invoked. Accordingly, claim 17 is allowable over Bal.

Claims 18 and 20-23 are allowable by virtue of their dependency on claim 17.

Claim 3 is not taught or suggested by the combination of Bal, Yoshiura, and Liu.

Claim 3

Dependent claim 3 recites:

The method as recited in claim 1, further comprising:

determining if the web page includes code to invoke a control object; and

deriving the digital signature and associating the digital signature with the web page only if the web page includes code to invoke a control object.

1 As described above, Bal describes determining a URL to which a browser  
2 running on a client computer is pointed and enabling a downloaded software  
3 program only if the URL to which the browser is pointed is an authorized URL.  
4 (Bal, Summary.) Bal does not describe “associating a digital signature with a web  
5 page,” as recited in claim 1, from which claim 3 depends. Furthermore, Bal does  
6 not describe, nor does the Office contend that Bal describes, “determining if the  
7 web page includes code to invoke a control object; and deriving the digital  
8 signature and associating the digital signature with the web page only if the web  
9 page includes code to invoke a control object,” as recited in claim 3.

10 Yoshiura describes a method for identifying a purchaser who purchased  
11 content from which an illegal copy was produced. (Yoshiura, Abstract.) Liu  
12 describes a server process for identifying a particular keyword in a web page, and  
13 then modifying the web page to enable secure download of executable code  
14 associated with the web page. Both Yoshiura and Liu fail to add any teaching to  
15 Bal regarding the features recited in claim 1. Namely, the combination of Bal,  
16 Yoshiura, and Liu fails to teach “associating a *digital signature with a web page*”  
17 and “executing at least a portion of the web page after *the digital signature* is  
18 authenticated,” as recited in claim 1.

19 Additionally, there is no suggestion to combine the teachings of Bal and  
20 Yoshiura. Yoshiura describes a method for identifying a purchaser who purchased  
21 content from which an illegal copy was produced. (Yoshiura, Abstract.) There is  
22 nothing in Yoshiura to suggest that identifying a purchaser of content has anything  
23 to do with authenticating access to executable code that may be invoked from a  
24 web page.

25

1 Furthermore, while Liu may disclose determining whether or not a web  
2 page includes code to invoke a control object, Liu does not teach or suggest using  
3 that information to determine whether or not to generate and associate a digital  
4 signature with the web page. Rather, Liu discloses using that information to  
5 determine whether or not to modify the web page to enable secure download of  
6 specific portions of executable code associated with the web page over a network.  
7 Liu describes processing that is performed in association with a web page that  
8 includes executable code that will need to be downloaded in order to be run. Liu  
9 does not suggest performing such processing in association with a web page that  
10 includes code that invokes a control object that may have already been  
11 downloaded. Accordingly, claim 3 is allowable over Bal in view of Yoshiura and  
12 further in view of Liu.

13  
14 *Claim 4 is not taught or suggested by the combination of Bal and Yoshiura.*

15  
16 *Claim 4*

17 Dependent claim 4 recites:

18  
19 The method as recited in claim 1, wherein the web page  
20 includes a confirmation module that is used by the electronic device  
21 to authenticate the digital signature.

22  
23 As described above, the combination of Bal and Yoshiura fails to teach the  
24 method as recited in claim 1. Specifically, the cited combination does not teach  
25 "associating a *digital signature with a web page*," and "delivering the web page to

1 an electronic device capable of authenticating the *digital signature* and executing  
2 at least a portion of the web page after *the digital signature* is authenticated,” as  
3 recited in claim 1. Furthermore, as noted previously, with respect to claim 3, there  
4 is no motivation provided in either reference that would suggest combining the  
5 teachings of Bal and Yoshiura. Accordingly, claim 4 is allowable over Bal in  
6 view of Yoshiura.

7  
8 *Claim 6 is not taught or suggested by the combination of Bal and Myer.*

9  
10 *Claim 6*

11 Dependent claim 6 recites:

12  
13 The method as recited in claim 1, wherein the web page is  
14 generated in an active server page (ASP) environment.

15  
16 Myer describes a system that includes a master controller and one or more  
17 devices (e.g., a TV, a VCR, a CD changer, etc.) such that the master controller can  
18 be used to control the devices. As described above, Bal does not teach or suggest  
19 the features recited in claim 1. Specifically, Bal does not teach or suggest  
20 “associating a digital signature with a web page.” Myer fails to add any teaching  
21 with respect to claim 1. Additionally, there is no motivation in either reference  
22 that would suggest combining the teachings of Bal and Myer. Therefore, and by  
23 virtue of its dependence on claim 1, claim 6 is allowable over Bal in view of Myer.  
24  
25

1 Claims 19, 32, and 34 are not taught or suggested by the combination of  
2 Bal and Renaud.

4 Claim 19

5 Dependent claim 19 recites:

7 The system as recited in claim 17, wherein the confirmation  
8 module is included in the control object.

9  
10 As described above, Bal does not disclose, teach, or suggest "a *web page*  
11 having a digital signature", as recited in claim 17, from which claim 19 depends.  
12 Rather, Bal discloses a *control object* having a digital signature, and examining a  
13 URL associated with a web page to determine whether or not the web page is  
14 authorized to invoke the control object. Bal does not disclose, teach, or suggest "a  
15 web page having a digital signature; an executable control object that may be  
16 invoked by [a] script in the web page; and a confirmation module configured to  
17 authenticate the digital signature to determine based on the authenticity of the  
18 digital signature, whether the control object should be invoked," as recited in  
19 independent claim 17.  
20

21 Furthermore, Renaud discloses methods, apparatuses, and products that  
22 reduce the computational demands placed on both source user computer systems  
23 and receiving user computer systems by requiring the implementation and the  
24 verification of only a single digital signature for an arbitrary number of data files.  
25



1 (Renaud, column 4, line 67 – column 5, line 4.) Renaud does not disclose, teach,  
2 or suggest a confirmation module included in a control object where the  
3 confirmation module is configured to authenticate a digital signature that is  
4 associated with a web page. Accordingly, the combination of Bal and Renaud  
5 does not teach or suggest the features of independent claim 17, from which  
6 claim 19 depends.

7 The Office cites Renaud column 4, lines 15-19 as disclosing “wherein the  
8 confirmation module is included in the control object,” as recited in claim 19. The  
9 cited portion of Renaud states:  
10

11  
12 “In another embodiment, computer-readable program code  
13 includes code for running the applet and code for determining  
14 whether the applet performs an action that triggers a security check.  
15 In another embodiment, code is included for use in establishing a  
16 secure connection with a remote site.”  
17

18  
19 The cited text in no way teaches or suggests a confirmation module  
20 included in a control object, as claimed. Accordingly, and by virtue of its  
21 dependence on claim 17, claim 19 is therefore allowable over Bal in view of  
22 Renaud.  
23  
24  
25

1        Claims 32 and 34

2        Independent claim 32 recites:

3  
4                A control object stored in a computer-readable medium,  
5        comprising computer-executable instructions that, when executed on  
6        a computer, perform the following:

7                authenticating a web page that invokes the control object,  
8        wherein the authenticating is performed based on a digital signature  
9        associated with the web page; and

10                executing a data-handling task on the computer if the web  
11        page is determined to be authentic.

12  
13                Claim 32 recites "a digital signature associated with the web page." As  
14        discussed above with reference to claim 3, neither Bal nor Renaud disclose, teach,  
15        or suggest a web page having an associated digital signature, nor authenticating a  
16        web page based on a digital signature that is associated with the web page.  
17        Accordingly, claim 32 is allowable over Bal in view of Renaud.

18                Claim 34 is allowable by virtue of its dependence on claim 32.  
19  
20  
21  
22  
23  
24  
25

1 Claims 27, 28, 30, and 31 are not taught or suggested by the combination  
2 of Bal and Liu.

3  
4 Claims 27, 28, 30, and 31

5 Independent claim 27 recites:

6  
7 A web browser contained on a computer-readable medium of  
8 a client computer, comprising computer-executable instructions that,  
9 when executed by the client computer, perform the following:

10 determining if a web page contains instructions to invoke a  
11 control object;

12 determining if the web page has an associated digital  
13 signature;

14 in an event that the web page has an associated digital  
15 signature, authenticating the web page using the digital signature;  
16 and

17 invoking the control object if the source of the web page is  
18 authenticated.

19  
20 Bal does not teach or suggest "determining if the web page has an  
21 associated digital signature," nor does Bal teach or suggest, "in an event that the  
22 web page has an associated digital signature, authenticating the web page using  
23 the digital signature." Liu does not add to the teaching of Bal regarding the cited  
24 claim features, nor does the Office claim that Liu adds to the teaching of Bal  
25

1 regarding the cited claim features. Rather, the Office merely refers to Liu as  
2 teaching "determining if the web page contains instructions to invoke a control  
3 object." (1/11/05 Office Action, p. 10.) Accordingly, claim 27 is allowable over  
4 Bal in view of Liu.

5 Claims 28, 30, and 31 are allowable by virtue of their dependence on  
6 claim 27.  
7  
8

9 **Conclusion**

10 The Office's basis and supporting rationale for the §102 rejection of claims  
11 1, 2, 5, 7-10, 17, 18, and 20-23 is not supported by the express teachings of Bal.  
12 The Office's basis and supporting rationale for the §103 rejections of claims 3, 4,  
13 6, 19, 32, 34, 27, 28, 30, and 31 are not supported by the cited combinations of  
14 Bal, Yoshiura, Liu, Myer, and Renaud. Applicant respectfully requests that the  
15 §102 and §103 rejections be overturned and that pending claims 1-10, 17-23 27,  
16 28, 30-32, and 34 be allowed to issue.  
17

18 Respectfully Submitted,  
19  
20

21 Dated: 6/21/05

22 By: Kayla D. Brant  
23 Kayla D. Brant  
24 Reg. No. 46,576  
25 (509) 324-9256 x 242

**(9) Claim Appendix**

1. method, comprising:  
associating a digital signature with a web page; and  
delivering the web page to an electronic device capable of authenticating  
the digital signature and executing at least a portion of the web page after the  
digital signature is authenticated.

2. The method as recited in claim 1, wherein the associating further  
comprises attaching the digital signature to the web page.

3. The method as recited in claim 1, further comprising:  
determining if the web page includes code to invoke a control object; and  
deriving the digital signature and associating the digital signature with the  
web page only if the web page includes code to invoke a control object.

4. The method as recited in claim 1, wherein the web page includes a  
confirmation module that is used by the electronic device to authenticate the  
digital signature.

5. The method as recited in claim 1, wherein the web page contains  
script that, when executed, invokes executable code that is executed on the  
electronic device executing the web page.

1           6.     The method as recited in claim 1, wherein the web page is generated  
2 in an active server page (ASP) environment.

3  
4           7.     A method, comprising:  
5           receiving a web page from a server, the web page containing executable  
6 script that, when executed, invokes a control object, the web page having a digital  
7 signature that can be used to identify a source of the web page;  
8           determining whether the source of the web page is authentic via the digital  
9 signature; and  
10          in an event that the source of the web page is authentic, displaying the web  
11 page and invoking the control object.

12  
13          8.     The method as recited in claim 7, further comprising:  
14          in an event that the source of the web page is not authentic, refusing to  
15 invoke the control object.

16  
17  
18          9.     The method as recited in claim 7, wherein the determining further  
19 comprises identifying the source of the web page.  
20  
21  
22  
23  
24  
25

1           10.    The method as recited in claim 7, further comprising:  
2           designating one or more authorized sources from which a web page that  
3           invokes a control object may be received; and  
4           executing script contained in the web page only if the determining indicates  
5           that the web page was received from one of the one or more authorized sources.

6  
7           17.    A system, comprising:  
8           a web browser configured to access a web page having a digital signature;  
9           a processor configured to execute script contained in the web page;  
10          an executable control object that may be invoked by the script in the web  
11          page and is executable on the processor; and  
12          a confirmation module configured to authenticate the digital signature to  
13          determine based on authenticity of the digital signature, whether the control object  
14          should be invoked.

15  
16          18.    The system as recited in claim 17, wherein the confirmation module  
17          is called by the control object.

18  
19          19.    The system as recited in claim 17, wherein the confirmation module  
20          is included in the control object.

21  
22          20.    The system as recited in claim 17, wherein the confirmation module  
23          is included in the web browser.

1           21.    The system as recited in claim 17, wherein the confirmation module  
2 is further configured to determine if the web page comes from a source that is  
3 authorized to invoke the control object and the control object is invoked only if the  
4 source of the web page is authorized to invoke the control object.

5  
6           22.    The system as recited in claim 17, wherein the confirmation module  
7 is called by the web page prior to the web page invoking the control object.

8  
9           23.    The system as recited in claim 17, wherein the digital signature  
10 module is not invoked if the web page does not have a digital signature.

11  
12           27.    A web browser contained on a computer-readable medium of a  
13 client computer, comprising computer-executable instructions that, when executed  
14 by the client computer, perform the following:

15               determining if a web page contains instructions to invoke a control object;  
16               determining if the web page has an associated digital signature;  
17               in an event that the web page has an associated digital signature,  
18 authenticating the web page using the digital signature; and  
19               invoking the control object if the source of the web page is authenticated.



1       28.    The web browser as recited in claim 27, further comprising:  
2       determining if the web page contains executable script to invoke a control  
3       object; and  
4       wherein the authenticating the web page further comprises authenticating  
5       the web page only if the web page contains executable script to invoke a control  
6       object.

7  
8       30.    The web browser as recited in claim 27, further comprising in an  
9       event that the web page does not have an associated digital signature, refusing to  
10      invoke the control object.

11  
12      31.    The web browser as recited in claim 27, further comprising  
13      instructions to determine if an authenticated web page comes from a source that is  
14      authorized to invoke the control object.

15  
16      32.    A control object stored in a computer-readable medium, comprising  
17      computer-executable instructions that, when executed on a computer, perform the  
18      following:

19      authenticating a web page that invokes the control object, wherein the  
20      authenticating is performed based on a digital signature associated with the web  
21      page; and

22      executing a data-handling task on the computer if the web page is  
23      determined to be authentic.

24  
25

1        34. The control object as recited in claim 32, further comprising  
2 instructions to determine if a source of the web page is authorized to invoke the  
3 data-handling task prior to executing the data-handling task.  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25